UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,504	01/27/2004	Kouhei Nadehara	Q79582	9262

23373 7590 04/01/2010

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
04/01/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sughrue@sughrue.com
PPROCESSING@SUGHRUE.COM
USPTO@SUGHRUE.COM

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/764,504	**Applicant(s)** NADEHARA, KOUHEI	
	Examiner RANDAL D. MORAN	**Art Unit** 2435	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 16 March 2010 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-14 and 16-20*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435

/Randal D. Moran/
Examiner, Art Unit 2435

Continuation of 11. does NOT place the application in condition for allowance because: Regarding Claims 1, applicant's arguments have been fully considered but are not persuasive. With respect to applicant's argument that the combination fails to teach a coefficient table providing first to fourth coefficients in response to said row index, applicant is directed to Takagi - column 26-lines 54-67, column 27-lines 1-5.1n response to applicant's argument that the reference uses RSA encryption as opposed to AES encryption, a recitation of the intended use (i.e. using AES encryption) of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. The actual encryption used does not distinguish the claims from the prior art as the prior teaches a coefficient table as recited in the claims.

With respect to applicant's argument that the combination fails to teach first to fourth field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively, applicant is directed to Van Buer - [0063][0064]. Van Buer discloses "The output of the exclusive-or circuit 114 of FIG. 2 can be a data block of the same width as was in block 11o, which can form an input 12o to a substitution circuit 122, as shown in more detail in FIG. 3. The input data block can be treated as a series of 8-bit octets A, B, C... to P in the ease of 198 bits, i.e., 16 octets, A, B, C... XH, in the ease of 192 bits, i.e., 24 octets and A, B, C... XP in the ease of 956 bits, i.e., 39 octets. Each octet can be used as an index into a substitution table (or inverse table during decryption), and the output into data block 194 can be the octet value in the table within the respective S-Box, e.g., $1... $16, i.e., the A, B, C... P in the substitution stage data block 124. Such a look-up table is referred to herein as an S-Box $1, $9, $3 • • • $16 or $94 or $39. Because the octets are independent in this step, maximum speed can be achieved by providing, e.g., 39 copies of the respective S-Boxes, $1... $32, for 256-bit Rijndael data blocks, or, e.g., 16 copies of the table $1... $16, for 128-bit AES, which can be implemented, e.g., as a read-only memory, and processing the entire block 19o in parallel, as illustrated in FIG. 3.

This substitution step can have the highest gate complexity in an implementation according to the present invention, since each table could contain 256 octets of data, 2048 bits in all. In applications where speed is less important, overall complexity could be reduced by implementing fewer copies of the tables, adding multiplexers and latches and using multiple clock cycles to perform substitution over different parts of the data block 12o in turn in each round." Van Buer discloses the output of the x-or circuit can form inputs into the substitution circuit and can be treated as a series of various octets. In response to applicant's argument that the combination doesn't explicitly teach the 1st to 4th coefficients, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). .